Security Compliance Categories

Administrative Procedures

Administrative procedures to guard data integrity, confidentiality, and availability are documented, formal practices used to manage the selection and execution of security measures to protect data and the conduct of personnel in relation to the protection of data. Administrative procedures can be seen in the table below.

Administrative Procedures to Protect Data

Requirement	Implementation
Certification	
Chain of trust partner agreement	
Formal mechanism for processing records	
Contingency plan *(all listed implementation features must be implemented)*	Applications and data criticality analysis. Data backup plan. Disaster recovery plan. Emergency mode operation plan. Testing and revision.
Information access control *(all listed implementation features must be implemented)*	Access authorization. Access establishment. Access modification.
Internal audit	
Personnel security *(all listed implementation features must be implemented)*	Assure supervision of maintenance personnel by authorized, knowledgeable person. Maintenance of record of access authorizations. Operating, and in some cases, maintenance personnel have proper access authorization. Personnel clearance procedure. Personnel security policy/procedure. System users, including maintenance personnel, trained in security.
Security configuration management *(all listed implementation features must be implemented)*	Documentation. Hardware/software installation and maintenance review and testing for security features. Inventory. Security Testing. Virus checking.
Security incident procedures *(all listed implementation features must be implemented)*	Report procedures. Response procedures.
Security management process *(all listed implementation features must be implemented)*	Risk analysis. Risk management. Sanction policy. Security policy.
Termination procedures *(all listed implementation features must be implemented)*	Combination locks changed. Removal from access lists. Removal of user account(s). Turn in keys, token, or cards that allow access.
Training *(all listed implementation features must be implemented)*	Awareness training for all personnel (including management).

	Periodic security reminders. User education concerning virus protection. User education in importance of monitoring log in success/failure and how to report discrepancies. User education in password management.

Physical Safeguards

Physical safeguards to guard data integrity, confidentiality, and availability relate to the protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. Physical safeguards also cover the use of locks, keys, and administrative measures used to control access to computer systems and facilities. Physical safeguards can be seen in the table below.

Physical Safeguards to Protect Data

Requirement	Implementation
Assigned security responsibility	
Media controls *(All listed implementation features must be implemented.)*	Access control. Accountability (tracking mechanism). Data backup. Data storage. Disposal.
Physical access controls (limited access) *(All listed implementation features must be implemented.)*	Disaster recovery. Emergency mode operation. Equipment control (into and out of site). Facility security plan. Procedures for verifying access authorizations prior to physical access. Maintenance records. Need-to-know procedures for personnel access. Sign-in for visitors and escort, if appropriate. Testing and revision.
Policy/guideline on work station use	
Secure workstation location	
Security awareness training	

Technical Security Services

Technical security services to guard data integrity, confidentiality, and availability include the processes that are put in place to protect and to control and monitor information access. Technical Security Services can be seen in the table below.

Technical Security Services to Protect Data

Requirement	Implementation
Access control *(The following implementation feature must be implemented: procedure for emergency access. In addition, at least one of the following three implementation features must be implemented:*	Context-based access. Encryption. Procedure for emergency access. Role-based access. User-based access.

Security Compliance Categories

context-based access, role-based access, user-based access. The use of Encryption is optional.)	
Audit controls	
Authorization control *(At least one of the listed implementation features must be implemented.)*	Role-based access. User-based access
Data Authentication	
Entity authentication *(The following implementation features must be implemented: automatic logoff, unique user identification. In addition, at least one of the other listed implementation features must be implemented.)*	Automatic logoff. Biometric. Password. PIN. Telephone callback. Token. Unique user identification.

Technical Security Mechanisms

Technical security mechanisms include the processes that are put in place to prevent unauthorized access to data that is transmitted over a communications network.

Technical Security Mechanisms to Protect Data

Requirement	Implementation
Communications/network controls *(If communications or networking is employed, the following implementation features must be implemented: integrity controls, message authentication. In addition, one of the following implementation features must be implemented: access controls, encryption. In addition, if using a network, the following four implementation features must be implemented: alarm, audit trail, entity authentication, event reporting.)*	Access controls. Alarm. Audit trail. Encryption. Entity authentication. Event reporting. Integrity controls. Message authentication.

The Electronic Signature Standard

In the electronic environment, the same legal weight associated with an original signature on a paper document may be needed for electronic data. Use of an electronic signature refers to the act of attaching a signature by electronic means. DHHS requires electronic signatures to include certain implementation features, specifically:

- Message integrity
- Nonrepudiation
- User authentication

No technically mature techniques provide the security service of non-repudiation in an open network environment, in the absence of trusted third parties, other than digital signature-based techniques. If electronic signatures are employed, DHHS requires that digital signature technology be used. The requirements of the electronic signature standard are defined in the table below.

Electronic Signature Standard Requirements

Security Compliance Categories

Requirement	Implementation
Digital signature *(If digital signature is employed, the following three implementation features must be implemented: message integrity, non-repudiation, user authentication. Other implementation features are optional.)*	Ability to add attributes. Continuity of signature capability. Counter signatures. Independent verifiability. Interoperability. Message integrity. Multiple signatures. Non-repudiation. Transportability. User authentication.